Die elektronische Gesundheitskarte

whitepaper

SICHERHEIT

Wie werden Gesundheitsdaten in Zukunft geschützt?

gematik GmbH · Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

INHALT

EINFÜHRUNG

Mit der Einführung der elektronischen Gesundheitskarte betritt Deutschland Neuland: Erstmals ist ein bundesweites Gesundheitsnetzwerk vorhanden, mit dessen Hilfe sich Krankenhäuser, Krankenkassen, Ärzte und Patienten auf das „digitale Zeitalter“ vorbereiten können.

Die Digitalisierung der medizinischen Versorgung gehört zu den anspruchsvollsten IT-Projekten weltweit. Experten rechnen mit über zehn Milliarden Datentransaktionen pro Jahr und schätzen das Datenaufkommen auf mehrere Dutzend Terabyte – und das ohne die Bilddaten, die durch moderne bildgebende Verfahren wie Computertomografie oder Magnetresonanztherapie zur Verfügung stehen.[1]

Neue technische Möglichkeiten werfen neue Fragen auf, vor allem im Bereich der Datensicherheit.

Neue Möglichkeiten

Die neuen technischen Möglichkeiten werfen auch neue Fragen auf, vor allem im Bereich der Datensicherheit.[2] Führt die Vernetzung dazu, dass durch kriminelle Angriffe, technische Schwachstellen oder menschliche Fehler Informationen über die Krankheiten des Inhabers einer elektronischen Gesundheitskarte von Unbefugten gelesen werden können? Kann eine ständig wachsende Anzahl von Bedrohungen in der Informationstechnik – etwa geknackte Passwörter, Trojaner oder ausgetrickste Sicherheitssysteme – die Vertraulichkeit der Informationen, die Arzt und Patient austauschen, gefährden?

Riesige Datenmengen

Bei einem System, das von riesigen Datenmengen und einer hohen Komplexität gekennzeichnet ist, spielt die Technik eine wichtige Rolle.[3] Wenn jährlich große Mengen Patientendaten in Computersystemen gespeichert und verarbeitet werden, wie lässt sich dann gewährleisten, dass man die ärztliche Schweigepflicht und das Bundesdatenschutzgesetz für jeden einzelnen dieser Datensätze einhalten kann?

Die Schreckensbilder vom „gläsernen Patienten“ oder vom „gläsernen Arzt“ zeigen, wie groß die Vertrauenslücke zwischen Bürger und Staat oder auch zwischen Mensch und Technik werden kann, wenn Gesundheitsdaten einem elektronisch vernetzten Informationssystem anvertraut werden.

Alleinstellungsmerkmal

Das Besondere an der elektronischen Gesundheitskarte und der dahinterliegenden Infrastruktur ist vor allem die Umsetzung einer

Sicherheitsphilosophie, die im digitalen Bereich bisher so noch nicht realisiert wurde. Die elektronische Gesundheitskarte ist das erste Großprojekt weltweit, bei dem die Zugriffsrechte auf die vorhandenen Daten allein in den Händen der Nutzer liegen. Im Prinzip ist dieses System vergleichbar mit einem Banksafe: Wer im geschützten Raum einer Bank einen privaten Safe mietet, kann darin etwas ablegen, ohne dass die Bank weiß, um was es sich handelt.

Die elektronische Gesundheitskarte ist das erste Großprojekt weltweit, bei dem die Zugriffsrechte auf die vorhandenen Daten in den Händen der Nutzer liegen.

Datenplattform

Dies bedeutet, dass die elektronische Gesundheitskarte vollständig anders mit Daten umgeht als bestehende Großsysteme für Datenerfassung, wie sie etwa bei Banken, Fluggesellschaften oder Behörden Verwendung finden. In diesen Systemen werden elektronische Daten so erfasst, dass Kunden oder Bürger keinen oder nur begrenzten Einfluss darauf haben, wer zu welcher Zeit Einsicht in ihre Daten hat. Mit der elektronischen Gesundheitskarte hingegen wird erstmalig eine Datenplattform geschaffen, die von der Dateneingabe bis zur Langzeitspeicherung so angelegt ist, dass der Karteninhaber zu jeder Zeit bestimmen und kontrollieren kann, was mit den gespeicherten Informationen passiert.

Wie funktioniert das?

Dieser Frage soll in vier Abschnitten nachgegangen werden.

Im ersten Abschnitt (S. 4 bis 15) geht es darum, den Begriff Sicherheit genauer zu definieren. Wann ist der Umgang mit digitalen Gesundheitsdaten sicher? Klare Regeln bestimmen, wann Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsdaten durch angemessene Maßnahmen ausreichend geschützt sind.

Verschlüsselung spielt bei der Gesundheitskarte die Hauptrolle.

Die Abschnitte zwei und drei (S. 16 bis 24) zeigen, mehr ins Detail gehend, dass die Verschlüsselung der digitalen Daten bei der Gesundheitskarte eine zentrale Rolle spielt. Es ist diese Verschlüsselung, die die neuartige Rechteverwaltung der Gesundheitsdaten überhaupt ermöglicht.

Abschnitt vier (S. 25 bis 29) bietet eine Übersicht über die Sicherheitsmaßnahmen beim Transport der Daten. Das Ziel ist es, vertrauliche Informationen in ein eigenes „Gesundheitsnetzwerk" innerhalb des weltweiten Datennetzes zu verschicken. Dieses Netzwerk besteht aus Innovationen der Telekommunikation und der Informatik – deshalb wird es „Telematikinfrastruktur" genannt.

1 GRUNDLAGEN DER SICHERHEIT

Wenn eine Ärztin Diagnosen, Therapievorschläge oder Vorerkrankungen eines Patienten auf dem Papier notiert, dann hat sie eine ungefähre Vorstellung davon, wodurch die Sicherheit dieser Daten bedroht sein kann.

Bei Informationen, die auf Papier oder lokalen Rechnern festgehalten werden, hat fast jeder eine intuitive Vorstellung davon, was Datensicherheit bedeutet.

Papier

So wäre es ein Verstoß gegen die Dokumentationspflicht des Arztes, wenn wichtige Papiere verloren gingen. Fahrlässig wäre es ebenfalls, wenn sich nicht feststellen ließe, ob Dokumente fehlen, von Unbefugten eingesehen oder gar kopiert wurden. Und bei unsachgemäßer Entsorgung von Dokumenten könnten diese in falsche Hände geraten. Also sorgt die sicherheitsbewusste Ärztin dafür, dass Archivschränke nicht allgemein zugänglich sind – indem sie etwa in einem separaten Raum aufgestellt oder mit Schlössern versehen werden. Akten werden nicht einfach entsorgt, sondern vernichtet, und Reservekopien der Verwaltung außerhalb der Praxis aufbewahrt.

Informationstechnologie

Ähnliches gilt für Praxen, in denen Informationstechnologie (IT) zum Einsatz kommt. Auch hier weiß der Arzt in etwa, was die Datensicherheit gefährdet: Alles, was zur Terminplanung oder zur Archivierung von Notizen oder Diagnosen auf dem Computer gespeichert wird, kann infolge von technischen Störungen, menschlichen Fehlern oder Vandalismus verloren gehen. Fehlt eine verlässliche Strategie für das Anlegen von Sicherheitskopien, können diese Informationen sogar unwiederbringlich verloren sein. Systeme, die mit einem drahtlosen Netzwerk oder dem Internet verbunden sind, können durch ungenügende Sicherheitsmaßnahmen Opfer von Hacker-Attacken werden.

Also wird auch hier dafür gesorgt, dass nicht jeder Zugang zu den Rechnersystemen hat – etwa durch Passwörter oder das Abkoppeln von Rechnern mit Patientendaten vom Internet. Außerdem achtet man auf eine verlässliche Strategie für die Erstellung verschlüsselter Sicherheitskopien, die außerhalb der Praxis aufbewahrt werden. Bei Lagerung, Transport und Entsorgung von Speichermedien werden die notwendigen Maßnahmen getroffen, die eine Vertraulichkeit der Daten sicherstellen.

Die Lage der IT-Sicherheit

Die kürzlich erschienene Studie „Die Lage der IT-Sicherheit in Deutschland 2007“ – herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI) – zeigt als positive Tendenz, dass Computeranwender zunehmend ein Bewusstsein für diese Art von Vorkeh-

rungen für den Datenschutz entwickeln. Allerdings stellt die Studie auch fest, dass sich immer noch viele professionelle Computeranwender zu wenig um das Thema Sicherheit kümmern.[4]

Lokale Vernetzungen

Ärzte, Rechtsanwälte und Angehörige sozialer Berufe dürfen vertrauliche Daten von Patienten, Mandanten beziehungsweise Klienten nicht ohne deren Einwilligung öffentlich machen.

Im Gesundheitsbereich führt das dazu, dass mancherorts lokale Vernetzungen eingeführt werden, bei denen das Niveau der Sicherheit und Kompatibilität ungenügend ist. Es mangelt vor allem an der Umsetzung einheitlicher Sicherheitsstandards, zum Beispiel solcher, die keinen unmittelbar erkennbaren Nutzen haben. Diese Standards sind aber essentiell, denn sie garantieren den langfristigen Schutz, die Verfügbarkeit und Vertraulichkeit von hochsensiblen Daten.

Die lokalen Vernetzungen sind auch deshalb bedenklich, da die aktuelle Gesetzeslage Vorstände und Geschäftsführer persönlich für Versäumnisse und mangelnde Risikovorsorge in der IT verantwortlich macht. Für Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe gelten gar Sonderregelungen im Strafgesetzbuch, die Freiheitsstrafen vorsehen, wenn vertrauliche Daten von Patienten, Mandanten bzw. Klienten ohne deren Einwilligung öffentlich gemacht werden (§ 203 StGB). Ein fahrlässiger Umgang mit Informationstechnik, auch in lokalen Netzwerken, kann diesen Tatbestand unter Umständen bereits erfüllen.

Bundesweite Vernetzung

Auch wenn Gesundheitsdaten den „geschützten Raum“ der einzelnen Praxen verlassen, ist es möglich, etwas über ihre Sicherheit auszusagen.

Sicherheit und Risiken der Informationsverarbeitung lassen sich in den oben beschriebenen Situationen – Papier und nicht vernetzte Informationstechnologie – relativ leicht erfassen. Aufgrund einiger weniger Beobachtungen und Eckdaten ist es möglich, das System als Ganzes zu überschauen und festzustellen, ob und in welchem Umfang unzumutbare Risiken vorliegen.

Wie sieht es nun bei einer bundesweiten Vernetzung der Informationstechnologie im Gesundheitssektor aus? Durch die Telematikinfrastruktur sind Ärzte, Patienten, Apotheken, Krankenhäuser und Krankenversicherungen miteinander verbunden. Dadurch verlassen die Gesundheitsdaten den „geschützten Raum“ der einzelnen Praxen. Ohne geeignete Gegenmaßnahmen würde damit ein Datenaustausch möglich werden zwischen Parteien, die nicht alles voneinander wissen dürfen, wie zum Beispiel Ärzte und Krankenversicherungen. Auch hat der Eigentümer oder Ersteller von Daten keine unmittelbare physische Kontrolle mehr über ihren Transport oder ihre Lagerung. Die handfesten Eigenschaften der Sicherheitsvorkehrungen vor Ort werden durch meist

unsichtbare Maßnahmen einer überregionalen Telematikinfrastruktur ersetzt. Diese Nichtwahrnehmbarkeit der Datenverarbeitung macht es den Beteiligten schwer, die Sicherheit zu beurteilen und dementsprechend zu handeln.

Telematikinfrastruktur

Trotzdem ist es auch hier durchaus möglich, etwas über die Datensicherheit auszusagen. Selbst wenn die Telematikinfrastruktur von vielen verschiedenen Menschen erstellt wurde und es keine direkte kausale Verbindung mehr gibt zwischen der Anwendung durch die Nutzer und der Leistung des Gesamtsystems, lässt sich anhand einiger klarer Regeln beschreiben, welchen Grundwerten das System im Hinblick auf die Sicherheit verpflichtet ist.[5] Die Hauptorientierung ist diese: Jeder Karteninhaber hat für seine Daten das Selbstbestimmungsrecht. Daraus lässt sich die angestrebte Sicherheit durch Zugangsberechtigung, Verschlüsselung, Datenvermeidung und Anpassung ableiten.

Sicherheit durch Zugangsberechtigung

So wie medizinische Praxen, Archivschränke und einzelne Rechner durch einen eingeschränkten Zugang geschützt sein können, spielt auch bei der elektronischen Gesundheitskarte die sogenannte „Zugangsberechtigung" eine zentrale Rolle. Sie sorgt dafür, dass nur die dazu berechtigten Personen oder Instanzen bestimmte Angebote in der Telematikinfrastruktur nutzen können. So ist genau festgelegt, wer welche Informationen über Patienten, Krankheitsverläufe oder generell gesundheitsbezogene Daten abfragen oder verändern darf.

Das „Zweikartenprinzip" sichert das Recht auf informationelle Selbstbestimmung des Patienten: Nur wenn Patient und Arzt sich einig sind, lassen sich Gesundheitsdaten aus dem System aufrufen.

Die Gesundheitskarte

Die am deutlichsten sichtbare Zugangsberechtigung zur Telematikinfrastruktur ist die elektronische Gesundheitskarte selbst, die jeder gesetzlich oder privat Versicherte in Deutschland erhält. Gleichzeitig bekommen auch alle Heilberufler und behandelnden Ärzte in Deutschland eine Karte, die „Heilberufsausweis" genannt wird.

Diese beiden Karten zusammen bieten die Gewähr, dass medizinische Daten nur nach Freigabe des Patienten von dem beauftragten Arzt eingetragen oder gelesen werden können. Da sowohl der Arzt als auch der Patient die Daten freigeben muss – das nennt man „Zweikartenprinzip" –, ist garantiert, dass nicht irgendjemand ohne Einwilligung des Versicherten auf medizinische Informationen zugreifen kann.

Jeder Versicherte entscheidet immer selbst über die Verwendung seiner Gesundheitsdaten.

Selbst entscheiden

Jeder Versicherte entscheidet also immer selbst über die Freigabe und Verwendung seiner Gesundheitsdaten. Dies beginnt bereits bei der Frage, ob überhaupt Gesundheitsdaten mit der elektronischen Gesundheitskarte gespeichert werden sollen. Im Sozialgesetzbuch ist dazu Folgendes festgelegt (§ 291a Abs. 3 Nr. 4 SGB V): Für die Karteninhaber gehören administrative Daten wie Name und Versichertennummer sowie die elektronische Verordnung zu den Pflichtanwendungen. Freiwillig ist die Speicherung aller anderen Daten, wie zum Beispiel Befunde, Diagnosen, Notfalldaten, Therapiemaßnahmen, Behandlungsberichte und Impfungen. Das heißt, dass jeder Patient selbst bestimmen kann, ob mit der elektronischen Gesundheitskarte neben den Pflichtdaten noch zusätzliche Informationen festgehalten werden.

Sicherheit durch Datenverschlüsselung

Die Methode, mittels derer das Lesen sensibler Daten durch unbefugte Dritte verhindert wird, heißt „kryptografische Verschlüsselung“. Dadurch wird eine Information so verändert, dass sie von Außenstehenden nicht mehr gelesen werden kann. Die Geschichte der Verschlüsselung reicht, wie der amerikanische Historiker David Kahn eindrucksvoll dargelegt hat, einige Jahrtausende zurück.[6] Sie ist geprägt von einem ständigen Wettlauf zwischen den Erfindern immer neuer Verschlüsselungsverfahren und ihren Widersachern, die alles daran setzten, die geheimen Botschaften zu entschlüsseln.

Die Geschichte ist geprägt von einem ständigen Wettlauf zwischen den Erfindern immer neuer Verschlüsselungsverfahren und ihren Widersachern, die alles daran setzten, diese zu knacken.

Schlüssel

Als Ergebnis dieses historischen Wettkampfes verfügen moderne kryptografische Methoden über die gemeinsame Eigenschaft, dass sie eine oder auch mehrere Zeichenreihen („Schlüssel“) für die Ver- oder Entschlüsselung von Informationen verwenden.

Über das Sicherheitsniveau dieser Schlüssel entscheiden vier Eigenschaften:

- **Die Komplexität:** Ein Schlüssel besteht aus einer willkürlichen Reihe von Zahlen. Je länger diese Zahlenreihe ist, desto sicherer ist auch die Verschlüsselung.
- **Die verwendete Verschlüsselungsmethode:** Die drei bekanntesten Methoden sind das symmetrische Verfahren, bei dem ein einziger

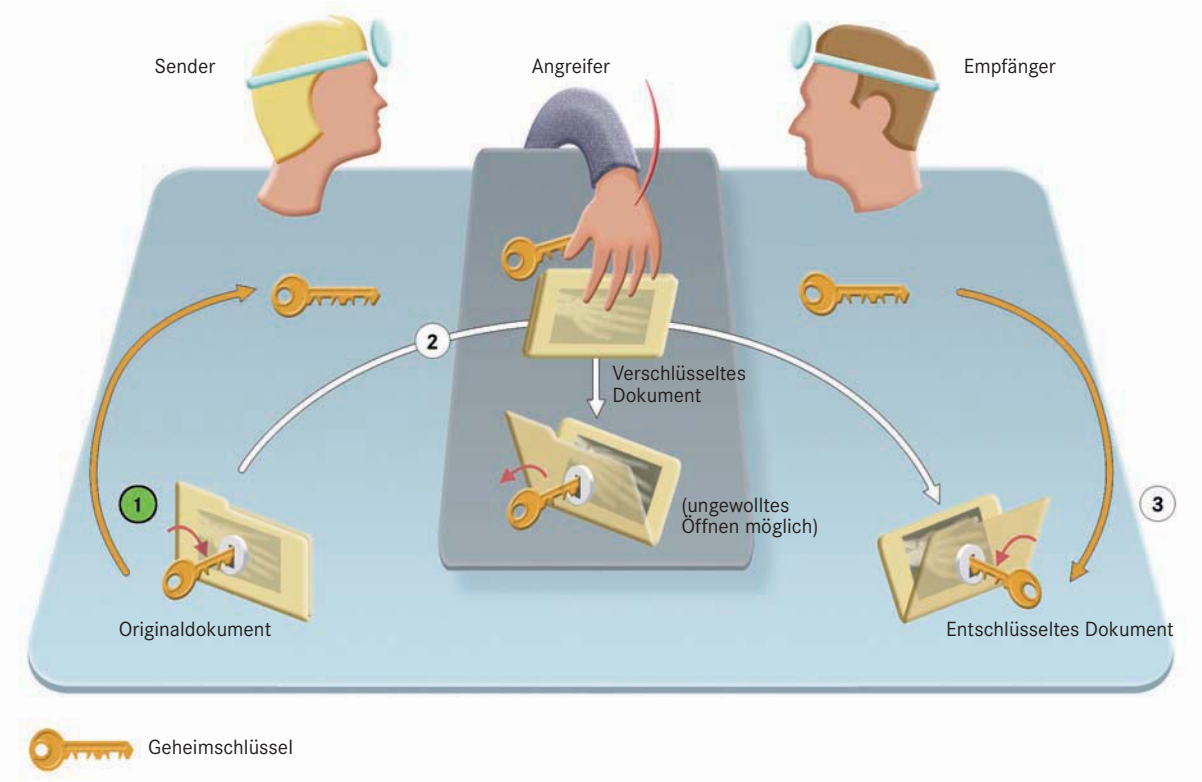


Abbildung 1a:
Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird ein geheimer Schlüssel zum Verschlüsseln der Nachricht verwendet ❶. Die für die Sicherheit wichtigste Frage ist: Wie transportiert der Sender (links) seinen geheimen Schlüssel zum Empfänger (rechts)? Der Empfänger braucht diesen Schlüssel, um die codierte Nachricht lesen zu können. Dabei werden ihm das verschlüsselte Dokument und der geheime Schlüssel über zwei getrennte Transportwege ❷ zugeschickt. Ein möglicher Angreifer (Mitte) kann sowohl die Nachricht als auch den Schlüssel abfangen. Verfügt er über beides, kann er das Originaldokument lesen. Der Empfänger merkt beim Öffnen der Nachricht ❸ nicht, ob der Schlüssel von einem Angreifer kopiert wurde.

Vorteil:
- Das Verfahren nimmt relativ wenig Rechenzeit in Anspruch und ist deshalb sehr schnell.

Nachteile:
- Sender und Empfänger müssen den Schlüssel sicher austauschen.
- Für den Versand des Schlüssels muss ein zusätzlicher Kanal geschaffen werden, der eine höhere Sicherheit bietet, als der Transportkanal für das verschlüsselte Dokument.

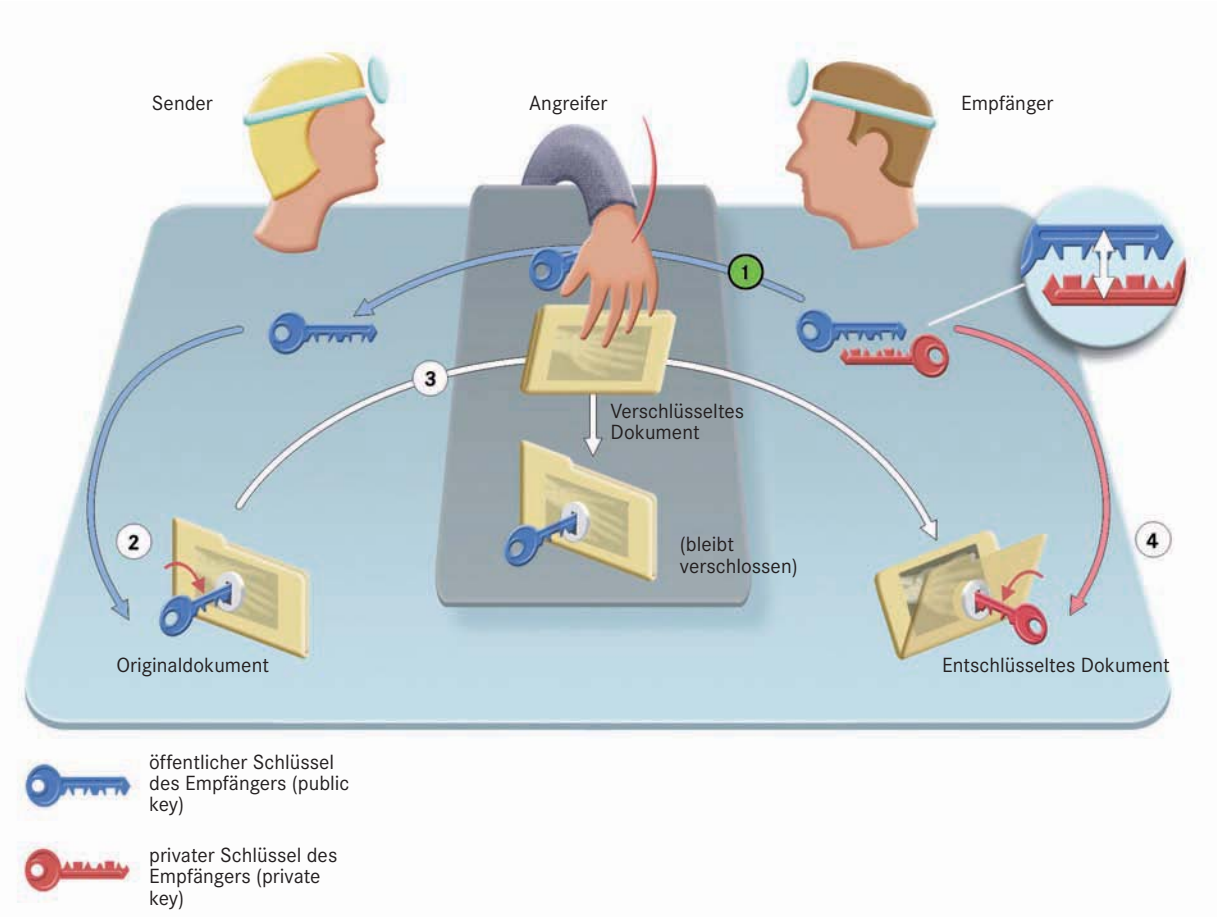


Abbildung 1b: Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung benutzen Sender (links) und Empfänger (rechts) das Schlüsselpaar des **Empfängers**. Dieses besteht aus einem öffentlichen und einem privaten Schlüssel: Mit dem öffentlichen Schlüssel können Dokumente ausschließlich codiert werden. Dechiffrieren lassen sie sich nur mit dem privaten Schlüssel. Die Bedingung für diese Art der Verschlüsselung ist, dass der Empfänger seinen öffentlichen Schlüssel allen zur Verfügung stellt, die ihm Dokumente zuschicken möchten ❶. Damit kann ein Sender nun ein Dokument zuschließen/verschlüsseln ❷. Das codierte Dokument erreicht über einen unsicheren Transportweg ❸ den Empfänger. Dass auch der Angreifer (Mitte) über den öffentlichen Schlüssel des Empfängers verfügt, beeinträchtigt die Sicherheit nicht – er kann damit die Nachricht nicht öffnen. Nur der Empfänger kann das verschlüsselte Dokument mit seinem privaten Schlüssel dechiffrieren ❹. So bleibt das Dokument für den Angreifer geheim.

Vorteile:

- Der Empfänger kann seinen öffentlichen Schlüssel jedem frei zur Verfügung stellen, denn damit lassen sich Dokumente nur verschlüsseln, nicht entschlüsseln.
- Der private Schlüssel muss nie über einen unsicheren Transportkanal verschickt werden, sondern bleibt immer beim Empfänger.

Nachteil:

- Das Verfahren ist relativ rechenintensiv.

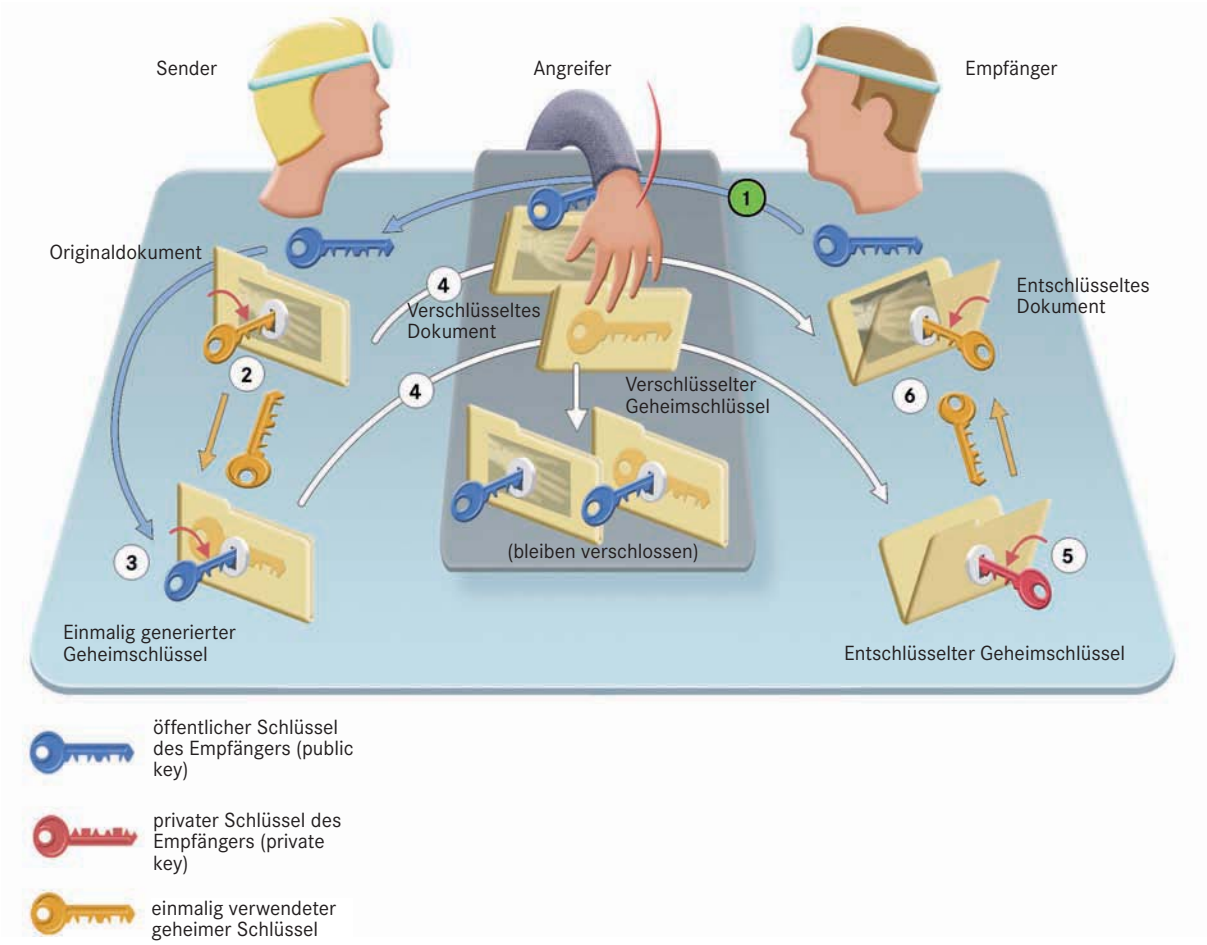


Abbildung 1c:
Gemischte (hybride) Verschlüsselung

Die hybride Verschlüsselung kombiniert die Vorteile der symmetrischen und der asymmetrischen Verschlüsselung. Als Vorbedingung gilt, dass der Empfänger (rechts) seinen öffentlichen Schlüssel dem Sender (links) zur Verfügung stellt ❶. Dann codiert der Sender das Originaldokument mit einem geheimen Schlüssel, den er selbst erzeugt hat ❷. Dieser geheime Schlüssel wird nun mit dem öffentlichen Schlüssel des Empfängers verschlüsselt ❸. Sowohl der codierte Schlüssel als auch das verschlüsselte Dokument gehen über einen Transportweg zum Empfänger ❹. Dass dabei der Angreifer beide Dokumente abfangen kann, beeinträchtigt die Sicherheit nicht, denn er verfügt nur über den öffentlichen Schlüssel des Empfängers. Damit bleiben alle Dokumente für ihn verschlossen. Der Empfänger verwendet anschließend seinen privaten Schlüssel, um den codierten Geheimschlüssel zu dechiffrieren ❺. Damit kann er das Originaldokument erfolgreich öffnen ❻.

Vorteile:

- Absender und Empfänger können den Geheimschlüssel austauschen, ohne dass er in die Hände des Angreifers fallen kann.
- Nicht alle Schlüssel müssen geheim bleiben, nur der private Schlüssel des Empfängers und der einmalig verwendete Geheimschlüssel.
- Der Empfänger darf seinen öffentlichen Schlüssel jedem frei zur Verfügung stellen.
- Das Verfahren nimmt relativ wenig Rechenzeit in Anspruch und ist deshalb sehr schnell.

Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung benutzt wird; das asymmetrische Verfahren, bei dem zwei getrennte, aber eng zusammenhängende Schlüssel für die Ver- und Entschlüsselung sorgen; und das hybride Verfahren, das eine Kombination aus den beiden vorherigen Verfahren ist > Abb. 1a, 1b, 1c.

- **Die Unabhängigkeit von der Geheimhaltung der gewählten Verschlüsselungsmethode:** Früher war die Geheimhaltung eines Verschlüsselungsverfahrens ein wesentlicher Bestandteil von dessen Sicherheit. Aber schon Ende des 19. Jahrhunderts zeigte der Linguist Auguste Kerckhoffs (1835–1903), dass die Sicherheit eines Verfahrens ganz unabhängig davon sein sollte, ob die Methode zur Verschlüsselung bekannt ist oder nicht.[7] So ist die Wahrung eines Geheimnisses nicht mehr von der Vertrauenswürdigkeit der involvierten Personen oder Instanzen abhängig, sondern nur noch von dem Verschlüsselungsverfahren selbst.
- **Die sichere Aufbewahrung der Schlüssel:** Die zur Dechiffrierung der Informationen verwendeten Zeichenfolgen müssen sehr sicher aufbewahrt werden.

Bei der elektronischen Gesundheitskarte spielt das „gemischte Verschlüsselungsverfahren“ eine Hauptrolle.

Gemischte Verschlüsselung

Bei der elektronischen Gesundheitskarte spielt das gemischte Verschlüsselungsverfahren eine Hauptrolle > Abb. 1c. Dieses Verfahren kombiniert optimal die Effizienz des symmetrischen Verfahrens mit den Vorteilen des asymmetrischen Verfahrens, sodass Sender und Empfänger keine Geheimschlüssel austauschen müssen. Statt eine ganze Botschaft asymmetrisch zu verschlüsseln – und im medizinischen Bereich kann es dabei um große Datenmengen gehen –, wodurch die Verschlüsselung rechenintensiv wird, muss nur noch der symmetrische Geheimschlüssel asymmetrisch verschlüsselt werden.

Sicherheit durch Datenvermeidung

Datenvermeidung sorgt dafür, dass nur die Daten verarbeitet werden, die für die Erfüllung einer Aufgabe absolut notwendig sind.

Neben Zugangsberechtigungen und kryptografischen Verschlüsselungen gehören Datensparsamkeit und Datenvermeidung zu jedem sicheren System. Das heißt, dass zu einer bestimmten Zeit und an einem bestimmten Ort nur solche Daten verarbeitet werden, die für die Erfüllung einer Aufgabe absolut notwendig sind. In der Praxis bedeutet das für die elektronische Gesundheitskarte, dass in der gesamten Infrastruktur konsequent drei Techniken zur Datenvermeidung Anwendung finden: **Datentrennung, Zweckbindung und Pseudonymisierung.**

- **Datentrennung:** Gesundheitsdaten werden in möglichst kleine Teile zerlegt und getrennt voneinander aufbewahrt. Nur wo es für die Nutzung unumgänglich ist, werden einzelne Informationen wieder zusammengefügt. Auch die personelle und organisatorische Datentrennung ist in der Telematikinfrastruktur der Gesundheitskarte ausdrücklich mitberücksichtigt. Das heißt, dass Personen oder Instanzen, die Adressdaten verwalten, keinen Zugang zu gesundheitsbezogenen Daten haben und umgekehrt.
- **Zweckbindung:** Vertrauliche Daten dienen in der gesamten Telematikinfrastruktur immer nur dem dafür vorgesehenen Zweck. Es ist im Sicherheitskonzept der Telematikinfrastruktur genauestens festgelegt, welche Art von Daten für welchen Zweck erforderlich ist.[8]
- **Pseudonymisierung:** Bei der elektronischen Gesundheitskarte werden Pflichtdaten, wie etwa die elektronischen Verordnungen, mit Pseudonymen versehen. Das wird gemacht, da der Versicherte in dem Bereich der Pflichtanwendungen besonders geschützt werden soll.

Datentrennung, Zweckbindung und Pseudonymisierung bei den Pflichtanwendungen verhindern also, dass Unbefugte aus Versehen oder mutwillig unzulässigen Zugriff auf miteinander verknüpfte Daten erhalten. Außerdem stellen sie effektive Gegenmaßnahmen gegen eine schwerwiegende Bedrohung vertraulicher Gesundheitsdaten dar: **die Profilbildung.**

Profilbildung

Profilbildung ermöglicht es, aus heterogenen Datensätzen, wie etwa aus Nutzungsstatistiken, umfassenden Datensammlungen oder unzusammenhängenden Datenfragmenten, neue sinnvolle Zusammenhänge herzustellen. Die Methode der Profilbildung wird heutzutage routinemäßig und mit steigender Raffinesse in der Informationstechnologie eingesetzt.

In der Telematikinfrastruktur ist Profilbildung durch strikte Anwendung oben genannter Methoden technisch weitgehend unmöglich. Hinzu kommt, dass alle Formen der statistischen Auswertung und das Erstellen von Zusammenhängen – etwa zwischen der Häufigkeit, mit der Patienten ihre Gesundheitskarte in einer bestimmten Praxis auslesen lassen, und der Art der Behandlung – gesetzlich verboten sind.

Keine der beteiligten Parteien kann auf Basis der gespeicherten Daten Zusatzwissen erwerben.

Das heißt, dass keine der beteiligten Parteien – sei es ein Arzt, eine Krankenversicherung, ein technischer Dienstleister oder auch der Gesetzgeber – auf Basis der gespeicherten Daten Zusatzwissen erwerben kann.

Sicherheit durch Anpassung

Wer eine Arztpraxis vor Einbruch sichert, macht das heutzutage anders als vor hundert Jahren. Sicherheit ist immer etwas, was sich verändert. Trotzdem gilt: Wer eine Praxis vor Einbruch sichert, kann davon ausgehen, dass die gewählten Maßnahmen (sofern sie sachkundig durchgeführt werden) diese für einige Jahre oder gar Jahrzehnte vor ungebetenen Eindringlingen schützt. In der digitalen Welt ist das anders.

Digitale Sicherheit ist eine wechselseitige Beziehung von Bedrohungen und Gefahrenabwehr, Risiko und Vertrauen, Hinterfragung und Konsensus in einem sich rasch verändernden IT-Umfeld.

Digitale Sicherheit

Digitale Sicherheit ist eine wechselseitige Beziehung von Bedrohungen und Gefahrenabwehr, Risiko und Vertrauen, Hinterfragung und Konsensus in einem sich rasch verändernden IT-Umfeld. In diesem Umfeld bestimmen im Wesentlichen zwei Faktoren die Datensicherheit: der **Mensch** und die **Technik**.

Für die Telematikinfrastruktur bedeutet dies, dass Datensicherheit von Anfang an als ein Prozess ständiger Anpassung – im Sinne von technischer Weiterentwicklung und dem Schutz gegen potenzielle Angreifer – verstanden wird. Die einzelnen Maßnahmen werden dabei für eine bestimmte Zeit geplant. Das System ist von der technischen Seite her auf fortdauernde Anpassung und Erweiterung ausgelegt. Aber auch organisatorische und personelle Aspekte sind mitberücksichtigt. Menschliches Versagen – Irrtümer, Nachlässigkeit oder ungenügende Schulung – gilt sogar als einer der wichtigsten Aspekte bei der Planung von Sicherheitskonzepten.

Die Telematikinfrastruktur verändert sich so schnell, wie es die aktuellen Dienste der Telematikinfrastruktur und die Möglichkeiten der Angreifer nötig machen.

Veränderungsbasis

Wie schnell sich die Telematikinfrastruktur verändert, wird unter anderem von den Entwicklungen im Bereich der kryptografischen Verschlüsselung bestimmt und davon, welche Dienste über die Telematikinfrastruktur angeboten werden.

Der Wettlauf zwischen den Erfindern neuer kryptografischer Verfahren und deren Angreifern wird in Deutschland – unter Berücksichtigung internationaler Entwicklungen – federführend vom Bundesamt für

Sicherheit in der Informationstechnik (BSI) beobachtet. Die Richtlinien, die daraus entstehen, haben für Behörden verbindlichen und für die gematik empfehlenden Charakter.[9]

Richtlinien

Die Richtlinien werden jährlich angepasst. Sie bieten einen Ausblick auf etwa sechs Jahre. Im Bereich der asymmetrischen Verschlüsselungsverfahren steigen die Anforderungen alle paar Jahre. Die Anforderungen an symmetrische Verfahren verändern sich in größeren Zeiträumen. Generell gilt, dass man über eine Zeitspanne von bis zu sechs Jahren mit einer genügend hohen Wahrscheinlichkeit Aussagen über die zu erwartenden Entwicklungen in den Verschlüsselungstechnologien machen kann.

Periodizität

Prozesshaftigkeit gehört zum Kern der Telematikinfrastruktur.

Die gewählte Periodizität von etwa sechs Jahren für die elektronische Gesundheitskarte kann sich also in Zukunft verändern, je nachdem, wie sich die Entwicklungen im Sicherheitsbereich gestalten. Diese Prozesshaftigkeit gehört zum Kern der Telematikinfrastruktur > Abb. 2.
Sie stellt hohe Anforderungen an Mensch und Technik, da immer wieder neue Konfigurationen im laufenden Betrieb geplant und getestet werden müssen.

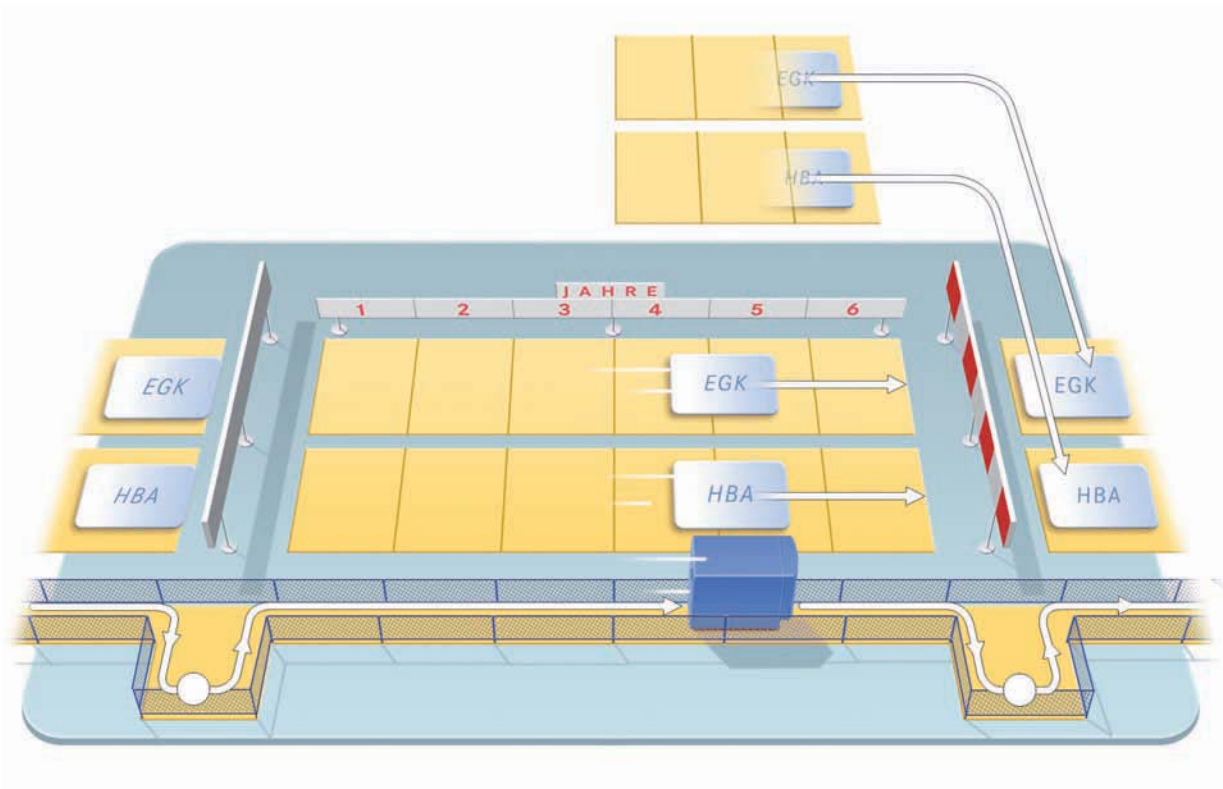


Abbildung 2:
Veränderung ist Teil der Telematikinfrastruktur

Die Infrastruktur der elektronischen Gesundheitskarte ist auf Veränderung ausgelegt. Jedes Jahr wird gemeinsam mit dem BSI geprüft, ob die verwendeten kryptografischen Mechanismen noch ausreichend sind oder gegebenenfalls ausgetauscht werden müssen. In diesem Fall bedeutet das nicht nur, dass beide Karten, die elektronische Gesundheitskarte und der Heilberufsausweis, erneuert werden, sondern auch, dass die Software und Hardware der Telematikinfrastruktur angepasst werden müssen. In jedem Fall werden die Karten alle sechs Jahre ausgetauscht. Auch unabhängig von kryptografischen Veränderungen wird die Telematikinfrastruktur fortlaufend verbessert. Dies erfordert eine langfristige Planung, die von der Spezifikation und Entwicklung, über Testmaßnahmen bis hin zur Inbetriebnahme reicht.

Da die Karte in der gesamten Infrastruktur eine Schlüsselrolle einnimmt, soll nun von ihr ausgehend der Informationsfluss im Telematik-Netzwerk betrachtet werden. Die Datenreise fängt bei der Prozessor-Chipkarte an. Danach geht es über das Kartenterminal zum Bindeglied zwischen der elektronischen Gesundheitskarte und der Telematikinfrastruktur, dem „Konnektor“. Sind die Daten einmal in der Telematikinfrastruktur angekommen, werden sie je nach Verwendungszweck in die dafür vorgesehenen Rechenzentren transportiert und für den Abruf bereitgehalten.

Die Prozessor-Chipkarte

Auf der Gesundheitskarte ist ein elektronischer Chip angebracht, der von außen genauso aussieht, wie der Chip der bisherigen Krankenversichertenkarte – ein goldenes, briefmarkengroßes Viereck. Trotz äußerlicher Ähnlichkeit handelt es sich dabei aber nicht mehr um einen reinen Speicherchip, sondern um eine Art miniaturisierten Computer, eine sogenannte „Smartcard“. Dies ist eine Prozessor-Chipkarte, die über einen Mikroprozessor, eine Speichereinheit und Kommunikationsschnittstellen verfügt. Ihre Rechenleistung ist vergleichbar mit dem Personalcomputer aus den späten 1980er-Jahren, allerdings ist der gesamte Rechner nun auf weniger als 25 Quadratmillimetern Halbleitermaterial untergebracht und wiegt nur den Bruchteil eines Gramms.

Die elektronische Gesundheitskarte verschlüsselt alle Daten mithilfe ihrer intelligenten Chipkarte, bevor sie in die Telematikinfrastruktur weitergeleitet werden.

Hauptfunktionen

Diese Prozessor-Chipkarte hat **zwei Hauptfunktionen**. **Erstens** fungiert sie als Authentifizierungswerkzeug. Dazu legt jeder Karteninhaber vor Erstverwendung eine persönliche Identifikationsnummer (PIN) nach Wahl fest. Die eigene PIN wird in verschlüsselter Form auf der Karte gespeichert. Danach blockiert der Prozessor jeden Zugriffsversuch auf die gespeicherten medizinischen Daten ohne korrekte PIN-Eingabe. Als Authentifizierungsinstanz protokolliert der Prozessor auch aktiv jeden Zugriff auf die Daten: Die letzten 50 Zugriffe werden in Kurzform auf der Karte gespeichert.

Verschlüsselungen

Die **zweite Funktion** der Prozessorkarte ist die Durchführung der kryptografischen Verschlüsselungen aller Gesundheitsdaten des Versicherten. Einmal verschlüsselt, sind die Daten geschützt, unabhängig

davon, wo sie sich gerade befinden. Alle Verschlüsselungen, die mit der Karte ausgeführt werden, sind vom Typ „hybride Verschlüsselung“ > Abb. 1c. Das heißt unter anderem, dass es für jede einzelne Gesundheitskarte ein eigenes Schlüsselpaar gibt, das aus einem öffentlichen und einem privaten Schlüsselteil besteht.

Der geheime Schlüssel

Die Vertraulichkeit der Gesundheitsdaten steht und fällt mit der Geheimhaltung des privaten Schlüssels.

Dass die gesundheitsrelevanten Informationen eines Versicherten geheim bleiben, steht und fällt mit der Geheimhaltung des privaten Schlüssels der elektronischen Gesundheitskarte. Deshalb hat man alle notwendigen Maßnahmen angewandt, um den Schutz des privaten Schlüssels des Patienten zu gewährleisten.

Komplexer Schlüssel

Erstens wird der Schlüssel so komplex wie möglich gewählt: Seine Länge beträgt im Moment **2048 Bit**. Wie sicher ist das? Im Jahr 2004 gelang es Forschern der Universität Bonn, einen 576-Bit-Schlüssel zu knacken. Es brauchte dazu einen Verbund von mehreren hundert Computern, die fast ein Jahr lang Tag und Nacht rechneten, um alle möglichen Schlüssel durchzuprobieren. Im Jahr danach gelang es dem Bundesamt für Sicherheit in der Informationstechnik, einen 640-Bit-Schlüssel aufzubrechen. Das ist bis heute der längste Schlüssel, der jemals geknackt wurde.

Denn mit jedem Bit, um das ein Schlüssel länger wird, vervielfacht sich die Zeit, die es dauert, ihn zu knacken. Dies beruht auf einem einfachen mathematischen Prinzip. Es ist leicht, zwei Zahlen miteinander zu multiplizieren, aber sehr schwer, aus dem Produkt wieder die ursprünglichen Zahlen herauszufinden. Bei der Rechenaufgabe „21 = 7 mal 3“ ist die Zerlegung noch einfach, aber bei großen Zahlen ist sie fast unmöglich.

Das Knacken eines 2048-Bit-Schlüssels würde mit dem derzeit leistungsfähigsten Rechner der Welt schätzungsweise mehrere Milliarden Jahre dauern.

Verschlüsselungsmethode

Zweitens: Die verwendete Verschlüsselungsmethode ist sehr sicher. Es handelt sich dabei um ein asymmetrisches Kryptosystem, das in den 1970er-Jahren entwickelt wurde. Dieses sogenannte „RSA-Verfahren“

wird vom Bundesamt für Sicherheit in der Informationstechnik als Kryptoalgorithmus für alle heutigen Karten empfohlen. Als Nachfolgetechnik ist das „Elliptische-Kurven-Kryptosystem“ (ECC) geplant. Dieses Verfahren ermöglicht eine nochmals gesteigerte Datensicherheit und eignet sich bei Anwendungen, bei denen die Speicher- oder Rechenkapazität naturgemäß begrenzt ist, wie etwa bei den Chipkarten der elektronischen Gesundheitskarte.

Geschützter Datenbereich

Drittens befindet sich der private Schlüssel in einem extrem stark geschützten Datenbereich der Chipkarte. Dieser Sicherheitsraum des Kartenspeichers ist eine Art digitaler Tresor, der sich von außerhalb der Karte grundsätzlich nicht auslesen lässt und den der Schlüssel niemals verlässt. Dieser digitale Tresor ist gegen alle Formen aktiver und passiver Lauschangriffe geschützt. Er ist zudem aufwendig gegen physikalische Manipulationen gesichert.

Nur der private Schlüssel jeder einzelnen elektronischen Gesundheitskarte kann Daten wieder lesbar machen – deshalb wird er sehr sicher auf der Karte selbst aufbewahrt.

Es ist für die Datensicherheit essentiell, dass der private Schlüssel nur einmal existiert. Deshalb müssen die Kartenhersteller nachweisen, dass sie keine Kopie davon besitzen, nachdem sie ihn bei der Kartenherstellung in den geschützten Datenbereich geschrieben haben.

Vollständige Offenlegung der Methode

Ein vierter Schutz des privaten Schlüssels besteht darin, dass seine Sicherheit nicht von der Geheimhaltung der gewählten Kartensorte oder der verwendeten Sicherheitsvorkehrungen auf der Karte abhängt. Hin und wieder werden außerhalb des Bereichs der elektronischen Gesundheitskarte Smartcard-Lösungen geknackt, obwohl man wahrscheinlich bei deren Erstellung davon ausging, dass die Geheimhaltung der verwendeten Technologie ausreichenden Schutz gegen Angreifer bieten würde. Beispiele finden sich etwa bei Smartcards, die im Pay-TV-Bereich, bei den öffentlichen Verkehrsbetrieben, in der Telekommunikation oder im Finanzwesen verwendet werden.

Angreifer dürfen alle technischen Details der elektronischen Gesundheitskarte kennen, nur der Inhalt des privaten Schlüssels auf der Karte bleibt streng geheim.

Deshalb erfüllen die für die elektronische Gesundheitskarte eingesetzten Chipkarten viel höhere Anforderungen als Chipkarten in den meisten anderen Bereichen. Alle technischen Details, ihre Stärken und theoretischen Angriffspunkte sind öffentlich bekannt.

Öffentliches Wissen unterstützt Sicherheit

Dieses öffentliche Wissen unterstützt die Sicherheit, schützt aber nicht vor allen Angriffen. Trotzdem gilt, dass die Offenheit die Sicherheit

Seit 2001 gab es keinen erfolgreichen Angriff gegen die von der elektronischen Gesundheitskarte verwendeten Chipkarten.

erheblich verbessert – denn der offene Umgang mit den verwendeten Technologien macht ihre Kontrolle und Pflege leichter. Zudem werden die Karten mit sehr großem Aufwand ständig geprüft, verbessert und zertifiziert. Diesen Maßnahmen ist es zu verdanken, dass die in der Gesundheitstelematik verwendeten Smartcards als das sicherste elektronische System außerhalb geschützter Rechenzentren gelten.[10] Seit Novellierung des Signaturgesetzes 2001, in dem die Rahmenbedingungen für elektronische Signaturen und Verschlüsselungen festgelegt sind, gab es keinen erfolgreichen Angriff gegen diese Art von zertifizierten Chipkarten.

3 DER KONNEKTOR

Der Konnektor lenkt alle Gesundheitsdaten so in die Telematikinfrastruktur, dass sie auf jeder Ebene gegen mögliche Angriffe geschützt sind.

Als Bindeglied zwischen dem Kartenprozessor der Gesundheitskarte, der Informationstechnologie in Arztpraxen, Krankenhäusern und Apotheken sowie der Telematikinfrastruktur fungiert der sogenannte „Konnektor".

Vom Aufbau her ist der Konnektor vergleichbar mit einem modernen, vollwertigen Rechner, der mit einer Reihe Sicherheitsvorkehrungen ausgestattet ist. So wird ein Betriebssystem verwendet, das sich in industriellen Anwendungen als sicher und zuverlässig bewährt hat.

Zertifiziert

Der Konnektor wird aufwendig getestet und zertifiziert.

Da der Konnektor in der Arztpraxis die Zugangsstelle zur Telematikinfrastruktur darstellt, wird er von der gematik und dem Bundesamt für Sicherheit in der Informationstechnik aufwendig getestet und zertifiziert. Alle Hersteller müssen nachweisen, dass die verwendeten Komponenten sowohl in der Hardware als auch in der Software vertrauenswürdig sind. Auch kann das Gerät durch regelmäßige Inspektionen vor Ort ständig überprüft und aktualisiert werden.

Gesundheitsdaten verschlüsseln

Bei einem Verschlüsselungsvorgang von Gesundheitsdaten arbeiten die elektronische Gesundheitskarte, der Heilberufsausweis und der Konnektor nahtlos zusammen > Abb. 3a. Zuerst authentifizieren sich sowohl Patient als auch Arzt durch die Eingabe der richtigen PIN: Der Patient muss die PIN nur einmal eingeben, nachdem er die Karte in der Arztpraxis in das Lesegerät gesteckt hat.

Verschlüsselung im Konnektor

Die medizinischen Daten – wie zum Beispiel Befunde, Diagnosen, Therapiemaßnahmen oder Röntgenbilder – werden danach aus den Rechnersystemen, die der Arzt verwendet, zum Konnektor geschickt.

Nun beginnt der Konnektor damit, diese Daten zu verschlüsseln. Dies geschieht mithilfe eines nach dem Zufallsprinzip generierten symmetrischen Geheimschlüssels. Dieses Verfahren geht schnell, da es sich um einen symmetrischen Schlüssel handelt und die Codierung mit dem leistungsfähigen Rechner des Konnektors durchgeführt wird.

Nachdem die Daten symmetrisch verschlüsselt wurden, wird nun der öffentliche, asymmetrische Schlüssel vom Kartenprozessor des Patienten abgerufen. Hiermit wird der geheime Schlüssel codiert.

So wird die Vertraulichkeit der Daten und des Geheimschlüssels gesichert und dann sorgt der Konnektor dafür, dass auch deren Integrität gewährleistet ist. Dazu generiert er anhand der medizinischen Daten eine Prüfsumme. Diese besteht aus einer Zahl, die eine Art Fingerabdruck von dem Originaldokument ergibt. Sie dient dazu, dass beim Lesen der Daten festgestellt werden kann, ob diese vollständig sind und nicht von Dritten verändert wurden.

Authentizität der Daten

Anschließend sichert der Konnektor noch die Authentizität der Daten. Dazu schickt er die Prüfsumme (den „Hash-Code“) an den Heilberufsausweis. Im Chip wird der Hash-Code elektronisch signiert und mit dem Zertifikat des Arztes versehen, das – wie eine Art Kopie eines Personalausweises – die Echtheit der Signatur belegt. Dieser Vorgang beweist, dass die Gesundheitsdaten echt sind, also wirklich dem Patienten gehören und vom Arzt erstellt wurden.

Danach bündelt der Konnektor alle Daten – die verschlüsselten Gesundheitsdaten, den codierten Geheimschlüssel, die Prüfsumme und die digitale Signatur – in einem digitalen Ordner.

Gesundheitsdaten entschlüsseln

Auch beim Entschlüsseln der Gesundheitsdaten arbeiten die elektronische Gesundheitskarte, der Heilberufsausweis und der Konnektor eng zusammen > Abb. 3b.

Abhörsicherer Datenkanal

Zuerst authentifizieren sich wieder sowohl der Patient als auch der Arzt. Aus der Telematikinfrastruktur wird vom Konnektor anschließend der gewünschte digitale Ordner abgefragt. Aus dem Ordner wird der codierte Geheimschlüssel *(gelb)* geholt und an die Prozessor-Chipkarte der elektronischen Gesundheitskarte geschickt. Einmal in der Recheneinheit angelangt, wird der Geheimschlüssel *(gelb)* vom privaten Schlüssel *(rot)* entschlüsselt. Danach wird der Geheimschlüssel durch eine abhörsichere Datenverbindung vom Kartenterminal zum Konnektor transportiert. Dieser dechiffriert mit dem Schlüssel anschließend die codierten Gesundheitsdaten und schickt diese zum Rechnersystem des Arztes. Nachdem die Entschlüsselung erfolgt ist, löscht der Konnektor den Geheimschlüssel.

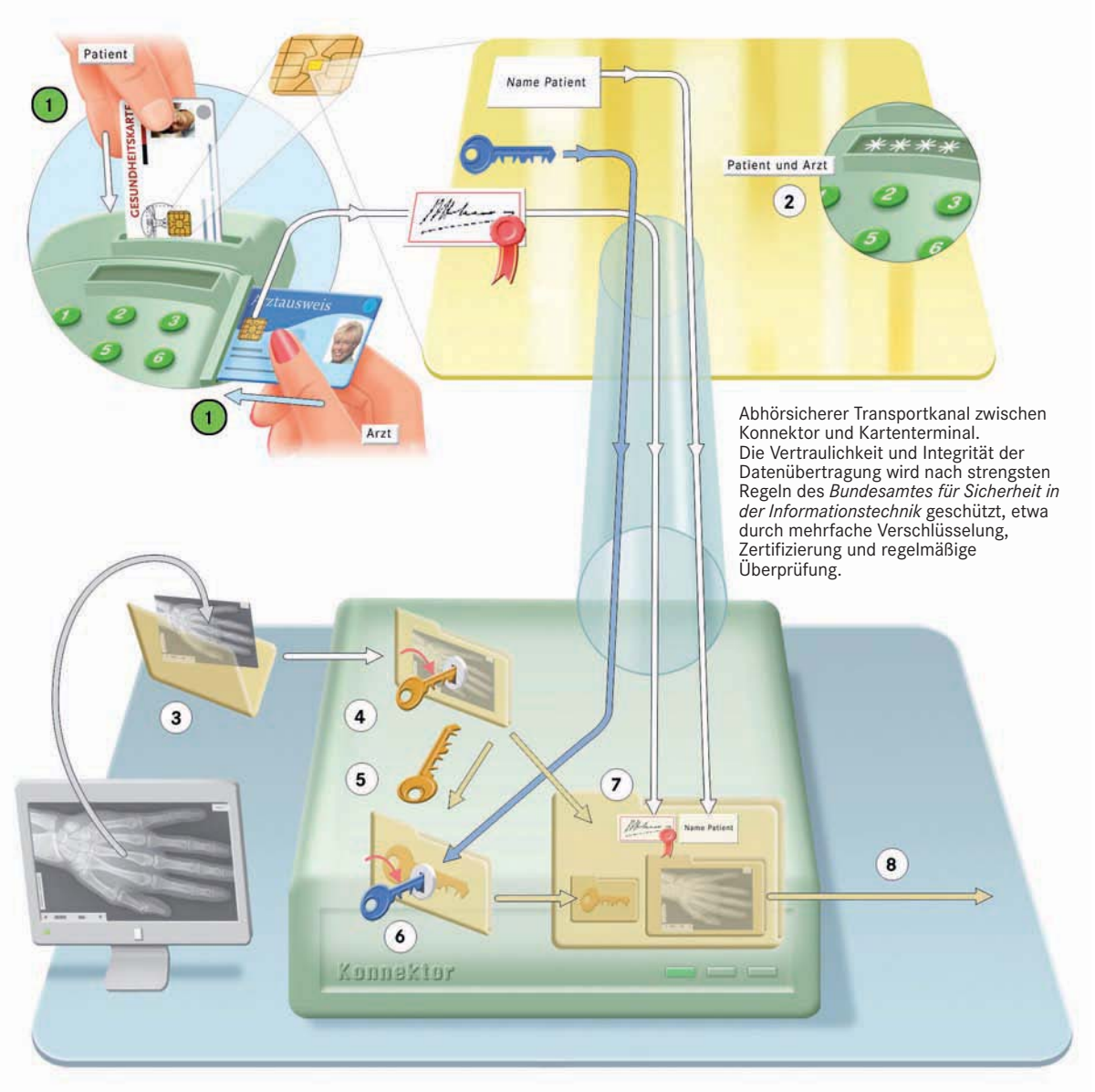


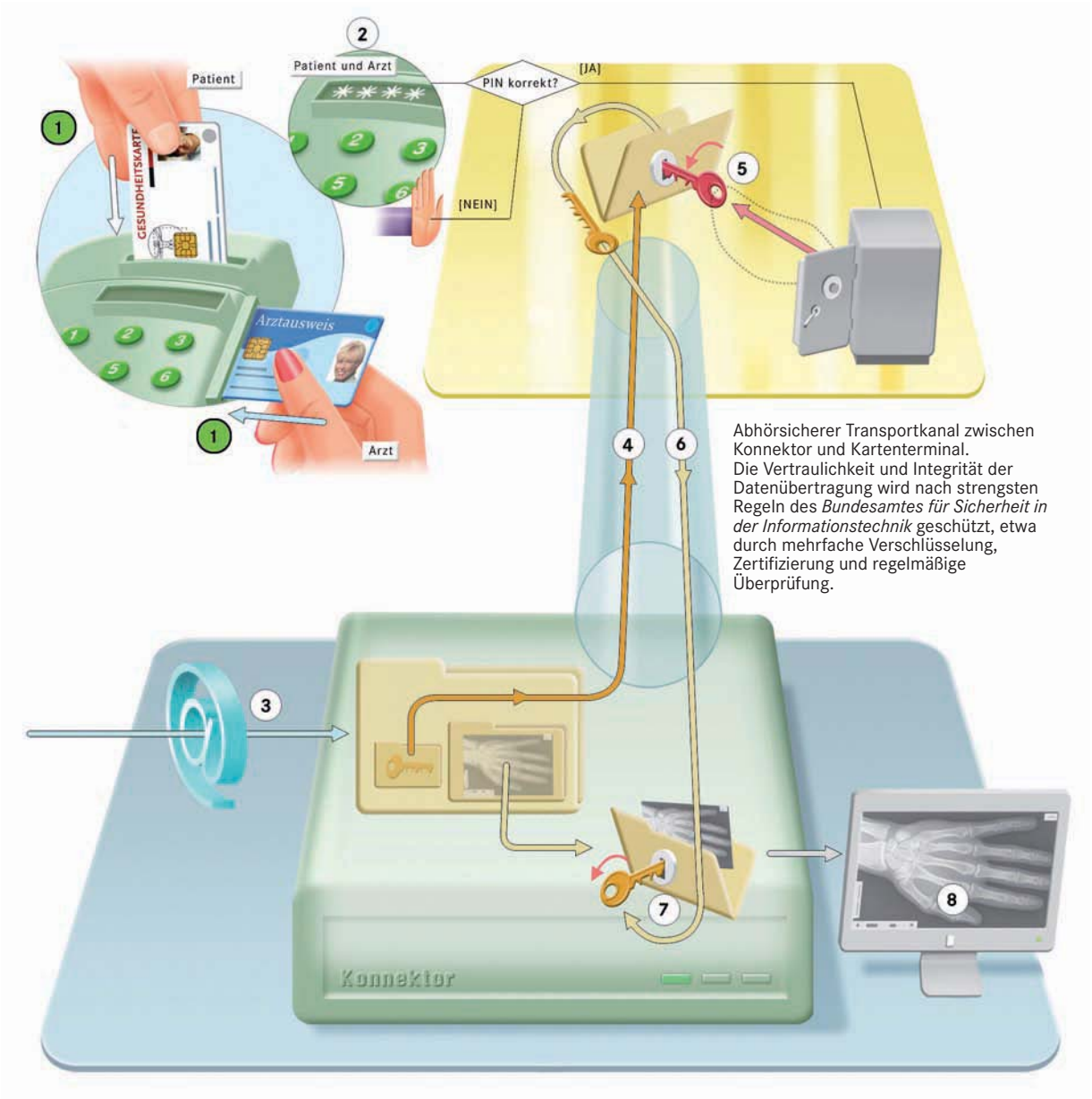
Abbildung 3a: Verschlüsseln von Gesundheitsdaten

Für die Verschlüsselung von Gesundheitsdaten greift das Zweikartenprinzip:

Nur wenn sich beide Karten im Kartenlesegerät befinden ❶ und bei beiden Karten die richtige PIN eingegeben wird ❷, können Daten in die Telematikinfrastruktur geschickt werden. Die Dechiffrierung folgt dem Prinzip der asymmetrischen Verschlüsselung > Abb. 1c.

Die Gesundheitsdaten werden zuerst zu dem Konnektor geschickt ❸.

Dieser generiert nach dem Zufallsprinzip nun einen einmalig zu verwendenden Geheimschlüssel und codiert damit symmetrisch die Gesundheitsdaten ❹. Der geheime Schlüssel wird mit dem öffentlichen Schlüssel der elektronischen Gesundheitskarte verschlüsselt ❺ ❻. Um sicherzustellen, dass die Daten wirklich zum Patienten gehören und vom Arzt signiert wurden, wird noch ein Zertifikat beigefügt ❼. Alle Daten werden danach in einen digitalen Ordner gepackt und zum Versand bereitgestellt ❽.



Abhörsicherer Transportkanal zwischen Konnektor und Kartenterminal.
Die Vertraulichkeit und Integrität der Datenübertragung wird nach strengsten Regeln des *Bundesamtes für Sicherheit in der Informationstechnik* geschützt, etwa durch mehrfache Verschlüsselung, Zertifizierung und regelmäßige Überprüfung.

Abbildung 3b: Entschlüsseln von Gesundheitsdaten

Zuerst müssen sich sowohl die elektronische Gesundheitskarte als auch der Heilberufsausweis im Kartenlesegerät befinden und mit gültiger PIN-Eingabe freigeschaltet werden ❶ ❷. Aus der Telematikinfrastruktur wird vom Konnektor der gewünschte digitale Ordner abgefragt ❸.
Aus dem Ordner wird der codierte Geheimschlüssel geholt und an die Prozessorkarte der elektronischen Gesundheitskarte geschickt ❹.
Die Entschlüsselung des Geheimschlüssels findet im Kartenprozessor statt ❺. Dabei verlässt der private Schlüssel des Karteninhabers niemals den Chip. Der dechiffrierte Geheimschlüssel wird durch den abhörsicheren Transportkanal zum Konnektor geschickt ❻, wonach sich die Gesundheitsdaten öffnen und darstellen lassen ❼ ❽.

Die Telematikinfrastruktur ist eine Art Datenautobahn, zu der nur Befugte Zutritt haben.

Hohes Sicherheitsniveau

Damit ist das Sicherheitsniveau der verschlüsselten Gesundheitsdaten so hoch, dass sie sogar in einem öffentlich zugänglichen Netzwerk zur Verfügung gestellt werden könnten, ohne dass sie sich in absehbarer Zeit entschlüsseln ließen.

In der Telematikinfrastruktur befinden sich die verschlüsselten Daten aber in einem mehrfach gesicherten Netzwerk. Es ist eine Art Datenautobahn, zu der nur Befugte Zutritt haben. Die Telematikinfrastruktur ist eine nach außen abgesicherte Infrastruktur, die sowohl gegen Angriffe als auch gegen technisches oder menschliches Versagen geschützt ist. Sie bietet somit die Gewähr, dass die Gesundheitsdaten auch unter erschwerten Bedingungen langfristig zur Verfügung stehen.

4 DER TRANSPORTKANAL

Gesundheitsdaten können lebensrettend sein: Diagnosen, Therapiemaßnahmen oder Behandlungsberichte sollten deshalb immer dort zur Verfügung stehen, wo sie helfen können, Menschenleben zu retten oder Krankheiten besser zu behandeln.

Gesundheitsdaten können lebensrettend sein. Deshalb werden sie nicht nur in einer Arztpraxis aufbewahrt, sondern zusätzlich vom Konnektor in die Rechner der Telematikinfrastruktur transportiert.

Deshalb werden die verschlüsselten Gesundheitsdaten nicht nur in der Arztpraxis aufbewahrt, sondern zusätzlich vom Konnektor in die Rechner der Telematikinfrastruktur transportiert. Danach stehen sie bundesweit allen Ärzten zur Verfügung, die vom Karteninhaber explizit zum Zugriff auf die Daten berechtigt worden sind.

Transportbedingungen

Der Transport von Gesundheitsdaten muss drei Bedingungen erfüllen:

- Erstens muss sichergestellt sein, dass der Sender der Daten weiß, dass der Empfänger auch wirklich derjenige ist, der er vorgibt zu sein (Authentifizierung). Zudem muss der Sender sicher sein können, dass der Empfänger auch berechtigt ist, die Daten entgegenzunehmen (Autorisierung).
- Zweitens muss der Transport abhörsicher sein. Denn auch wenn die Gesundheitsdaten selbst so verschlüsselt sind, dass sie von niemandem gelesen werden können – bereits das bloße Verschicken von verschlüsselten Daten könnte Angriffsflächen für Profilbildungen bieten.
- Drittens muss gewährleistet sein, dass die Gesundheitsdaten auch tatsächlich immer zur Verfügung stehen, wenn sie gebraucht werden. Das Transportsystem muss also dafür sorgen, dass es gesichert ist gegen alle möglichen Störungen. Dazu muss es sich selbst auch aktiv gegen Angriffe schützen. Etwa gegen solche, die das Ziel haben, einen oder mehrere Dienste der Telematikinfrastruktur arbeitsunfähig zu machen.

Die Telematikinfrastruktur bietet intelligente Datensicherheit.

Datenpakete

Für die Authentifizierung und Authentisierung sorgen die Anwendungen des Systems. Dabei kann es sich um ein Programm zur Verwaltung der Stammdaten von Patienten handeln, um eine Praxisverwaltungssoftware oder auch um einen Fachdienst zur Speicherung von elektronischen Rezepten.

Der Transport von Gesundheitsdaten erfüllt strenge Kriterien.

Diese Programme teilen die bereits verschlüsselten Gesundheitsdaten in kleinere Pakete, wovon jedes einzelne nochmals verschlüsselt wird. So ist gewährleistet, dass die Daten in der Telematikinfrastruktur

nur zwischen Teilnehmern verschickt werden, die sich gegenseitig identifiziert und auf Berechtigungen hin kontrolliert haben. Damit findet eine Nachrichtenauthentifikation auf Anwendungsebene statt, was eine Garantie für eine sichere Endpunkt-zu-Endpunkt-Kommunikation darstellt.

Für den abhörsicheren Transportkanal sorgt der Konnektor. Er teilt die verschlüsselten Gesundheitsdaten, die auf der Anwendungsebene in kleine Pakete geteilt und verschlüsselt wurden, in noch kleinere Pakete ein. Diese werden anschließend erneut einzeln verschlüsselt, bevor sie in die Telematikinfrastruktur gehen > Abb. 4.

„Firewall"-Funktion

Der Konnektor sorgt nicht nur für einen abhörsicheren Transportkanal, sondern auch dafür, dass keine Pakete unbefugt dort hineingeraten können. Dazu kontrolliert der Konnektor den ein- und ausgehenden Datenverkehr. Durch diese „Firewall"-Funktion wird zudem sichergestellt, dass angeschlossene medizinische Systeme nicht durch Daten aus dem Netz oder aus dem Internet infiziert oder beschädigt werden können. Alle potenziellen Sicherheitsvorfälle werden dabei protokolliert.

Auf diese Art und Weise sind die Integrität, Authentizität und Vertraulichkeit des Transportkanals gewährleistet.

Der Broker

Die von der Arztpraxis aus verschickten Datenpakete werden auf der zentralen Seite der Telematikinfrastruktur vom sogenannten „Broker" empfangen. Der Broker fungiert als Vermittler zwischen dem Konnektor und den vernetzten Rechenzentren. Dabei übernimmt er verschiedene Funktionen.

- **Erstens die Authentifizierung:** Er kontrolliert jedes eingehende Datenpaket darauf, ob es von einem zugelassenen, zertifizierten und geprüften Konnektor in einer berechtigten Institution verschickt wurde. Dazu vergleicht der Broker Absender-Signaturen auf den Datenpaketen mit fortlaufend aktualisierten „weißen" und „schwarzen" Listen von zugelassenen und gesperrten Konnektoren.
- **Zweitens die Verfügbarkeit:** Der Broker schützt aktiv gegen Angriffe, die das Ziel haben, das System zu überlasten oder auf sonstige Art dafür zu sorgen, dass Gesundheitsdaten nicht mehr dort zur

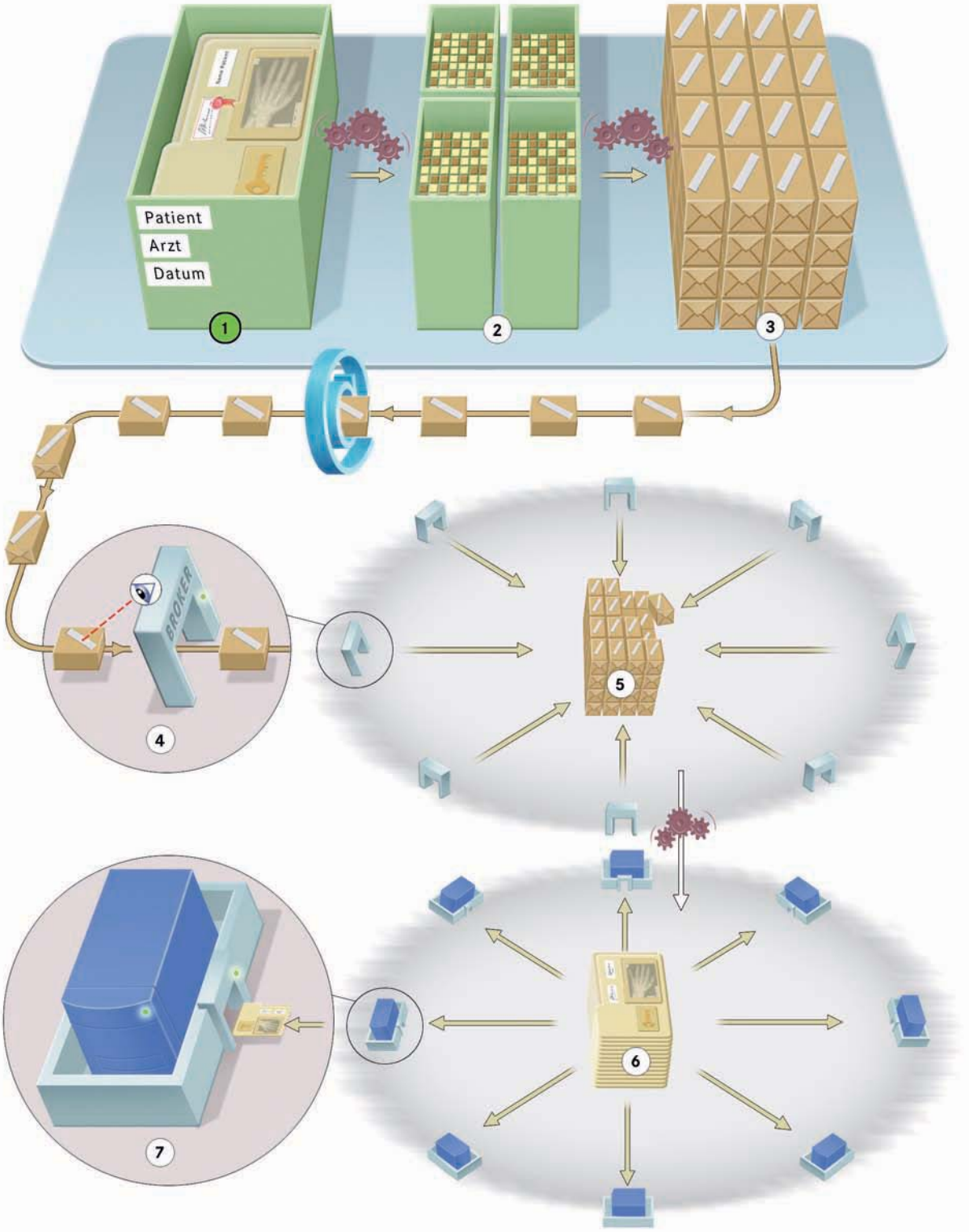


Abbildung 4:
Datentransport in die Telematikinfrastruktur

Die verschlüsselten Gesundheitsdaten ❶ werden für den Datentransport zweimal in Datenpakete geteilt und anschließend verschlüsselt: zuerst auf Anwendungsebene mit dem „Secure Sockets Layer"-Protokoll (SSL) ❷. Mittels des „Internet Protocol Security"-Verfahrens (IP sec) werden die SSL-Datenpakete danach nochmals in kleinere Transportpakete geteilt ❸. Die Datenpakete werden von dem Broker kontrolliert und entgegengenommen ❹. In der Telematikinfrastruktur werden sie wieder zugeordnet ❺, zusammengesetzt ❻ und in Rechenzentren abgelegt ❼.

Verfügung gestellt werden können, wo sie gebraucht werden (sogenannte „Denial of Service“-Angriffe).

Aufgrund ihrer zentralen Rolle werden hohe Anforderungen an die Sicherheit, Verfügbarkeit und Skalierbarkeit von Brokern gestellt. Jeder Broker hat eine interne Notfallplanung und entsprechende Tests werden regelmäßig durchgeführt.

Eine spezielle Herausforderung an dieses Kontinuitätsmanagement besteht darin, dass die gesamte Telematikinfrastruktur sich permanent verändert. Das heißt, dass immer wieder neue Software-Versionen oder Korrekturen kurzfristig eingespielt werden müssen. Das erfordert eine schnelle und flexible Technik sowohl des Brokers als auch aller Beteiligten.

Der Auditdienst

Mit dem Auditdienst hat jeder Karteninhaber die lückenlose Kontrolle darüber, wer, wann, wo Zugriff auf seine Daten hatte.

Wie kann der Karteninhaber nun überprüfen, wann, von wem und wie ein Zugriff auf seine Daten erfolgte? Ist er dazu auf das Vertrauen in die Telematikinfrastruktur angewiesen, oder gibt es eine Möglichkeit der eigenständigen Kontrolle?

Jeder kann seine Datenvorgänge überprüfen

Der sogenannte „Auditdienst“ („auditio“ bedeutet im Lateinischen „anhören“) sorgt dafür, dass alle Zugriffe auf Patientendaten in einem Protokoll festgehalten werden. Damit kann nachvollzogen werden, wer zu welchem Zeitpunkt welche Gesundheitsdaten aufgerufen oder gespeichert hat.

Die Protokollierung folgt immer dem Prinzip der Datensparsamkeit. Das heißt unter anderem, dass medizinische Daten in den Protokollen nie – auch nicht verschlüsselt – gespeichert werden. Zudem erfüllen die Protokolle grundsätzlich alle gesetzlichen Anforderungen wie etwa die des Telekommunikationsgesetzes, des Telemediengesetzes und des Bundesdatenschutzgesetzes.

Private Protokolldaten

Um zu gewährleisten, dass Protokolldaten nie von Dritten gelesen werden können, sondern nur vom Karteninhaber selbst, werden sie mit dem öffentlichen Schlüssel des Karteninhabers verschlüsselt. Nicht einmal Systemadministratoren haben Zugang zu den Auditdaten.

So kann jeder Karteninhaber – und nur er – mit eigenen Augen überprüfen:

- **welche** Ereignisse mit seinen Daten in der Telematikinfrastruktur stattgefunden haben
- **wer** diese Ereignisse veranlasst hat
- **wo** und wann diese Ereignisse stattgefunden haben.

Individuelle Kontrolle

Der Auditdienst ermöglicht also eine Art individueller Kontrolle, die essentiell ist für die Patientensouveränität. Denn mit diesem Zugriffsprotokoll kann der Karteninhaber wirklich nachvollziehen, ob es zu einem ungewollten Zugriff auf seine Daten gekommen ist – sei es mit der elektronischen Gesundheitskarte selbst, in einem Konnektor oder einem Broker.

Da der Auditdienst zum grundlegenden Patientenrecht gehört, entspricht er den höchsten Sicherheitsanforderungen. Es darf zum Beispiel nie vorkommen, dass Daten zentral abgerufen werden, ohne dass darüber ein Nachweis entsteht. Sollte ein Auditdienst zeitweilig nicht erreichbar sein, dann wird die Protokollierung auf der elektronischen Gesundheitskarte selbst durchgeführt.

Auch ist genauestens vorgeschrieben, welche Daten wann und wo protokolliert werden müssen, und wie lange sie aufbewahrt werden dürfen. Die Protokolldaten werden in der gesamten Telematikinfrastruktur immer nur so übertragen und gespeichert, dass eine Zusammenführung von Ereignissen unterschiedlicher Versicherter oder eine Profilbildung durch Dritte unmöglich ist.

Insgesamt gilt, dass die Verfügbarkeit und Erreichbarkeit des Auditdienstes zu den Kernfunktionen der Telematikinfrastruktur gehört. Deshalb verwendet man, genauso wie bei den Brokern, für den Auditdienst nur zertifizierte Komponenten, die laufend überprüft werden.

Medizinische Daten sind ein kostbares Gut. Die Telematikinfrastuktur bietet einen Rahmen, um ihren elektronischen Transport so sicher wie möglich zu gestalten. Schon heute trägt jede Ärztin und jeder Arzt eine hohe persönliche Verantwortung für den sicheren Umgang mit medizinischen Daten. Künftig werden sie diese mit den Versicherten teilen. Denn die maßgebliche Verantwortung für die Nutzung der Gesundheitsdaten liegt mit der Telematikinfrastruktur immer in den Händen der Karteninhaber.

Telematikinfrastruktur in der Praxis

Was passiert, wenn die Telematikinfrastruktur in der Praxis eingesetzt wird? Jedes sichere Informationssystem kennt bei der Umsetzung eine umfangreiche Liste mit denkbaren, oft technisch komplexen Bedrohungs- und Risikoszenarien. Gibt es nicht doch potenzielle Störungen oder künftige Angriffe, wodurch die Sicherheit in Gefahr geraten könnte?

Hier gilt tatsächlich, dass Sicherheit und ihre Anforderungen laufend fortgeschrieben werden. Gerade deswegen ist die Telematikinfrastruktur so entwickelt, dass sie steigende Anforderungen an die Systemsicherheit im laufenden Betrieb immer berücksichtigen kann.

Starke Verschlüsselung der Gesundheitsdaten

Bei allen technischen Fragen und möglichen Bedrohungsszenarien für die Telematikinfrastruktur sollte man aber immer im Auge behalten, dass die Verschlüsselung aller Gesundheitsdaten mithilfe der Prozessor-Chipkarte durchgeführt wird.

Die Verschlüsselung der Gesundheitsdaten mithilfe der Prozessor-Chipkarte und des Konnektors ist so sicher, dass sie auch dann greift, wenn sich die verschlüsselten Gesundheitsdaten außerhalb der physischen Kontrolle des Eigentümers befinden.

Diese Verschlüsselung allein bietet die Sicherheit, dass unerlaubtes Einsehen der Daten nicht möglich ist. Der Schutz greift auch dann, wenn die verschlüsselten Daten sich außerhalb des direkten Einflusses des Dateneigentümers befinden.

Sogar wenn digitale Gesundheitsdaten in die Hände von Unbefugten fallen oder in die Öffentlichkeit geraten sollten – wie bereits in den USA, in Großbritannien und in den Niederlanden geschehen –, sind sie mit der Verschlüsselung der elektronischen Gesundheitskarte gegen unbefugtes Lesen geschützt.

Trotzdem sollte man sich den vielen möglichen Szenarien und Bedrohungen – nicht nur den kurzfristigen, sondern auch solchen, die in zehn oder zwanzig Jahren auftauchen könnten – mit Sorgfalt und großer Offenheit widmen. Denn es geht letztendlich um nicht weniger als die Garantie der langfristigen Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von äußerst schützenswerten Daten.

Langfristige Datensicherheit

Gegenüber Einzellösungen zeigt sich die Telematikinfrastruktur als Plattform, die eine sehr hohe und langfristige Datensicherheit mit system- und regionenübergreifender Kompatibilität vereint. Das Niveau der Datensicherheit geht bereits heute über das bestehender Lösungen hinaus. Es sind eine Reihe von Sicherheitsstandards entwickelt und getestet worden, die sich dadurch auszeichnen, dass sie den gesamten Datenweg – von der Entstehung bis zur Langzeitarchivierung der Daten – berücksichtigen.

Allgemeines Modell für vertrauliche Daten

Vor allem die konsequente Umsetzung des Rechts auf informationelle Selbstbestimmung des Patienten macht die Telematikinfrastruktur zu einer notwendigen Voraussetzung für eine effektive Anwendung moderner Informations- und Kommunikationstechniken im deutschen Gesundheitswesen. Diese Umsetzung ist nicht nur für Gesundheitsdaten eine wichtige Innovation, sondern sie kann auch als Modell für den langfristigen Umgang mit vertraulichen Daten im „digitalen Zeitalter“ dienen.

ANMERKUNGEN

1 Zipfel, Martin. *Elektronische Patientenakte ‚gläserner Patient' oder der Weg aus der Krise des Gesundheitswesens?:* GRIN Verlag, 2007. Schug, S. H. *European and International Perspectives on Telematics in Healthcare*, IOS Press, 2001; Marsh, Andy; Grandinetti, Lucio; Kauranne, Tuomo. *Advanced Infrastructures for Future Healthcare*, IOS Press, 2000.

2 Blobel, Bernd (Hrsg.). *Datenschutz in medizinischen Informationssystemen*, Braunschweig: Vieweg, 1995; Eberspächer, Jörg. *Sichere Daten, sichere Kommunikation: Datenschutz und Datensicherheit in Telekommunikations- und Informationssystemen = Secure information, secure communication*, Berlin: Springer, 1994; Iwansky, Patrizia: *Datenschutzrechtliche Probleme von Chipkarten am Beispiel der geplanten Patientenkarte unter besonderer Berücksichtigung der europäischen Entwicklung*, Berlin: Mensch und Buch-Verlag, 1999; Haas, Peter. *Gesundheitstelematik: Grundlagen, Anwendungen, Potenziale*, Berlin, Heidelberg, New York: Springer, 2006; Kraft, Dennis. *Telematik im Gesundheitswesen: Vertragsarzt- und datenschutzrechtliche Aspekte*, Wiesbaden: DUV, 2003; Krzysztof Zieliński; Mariusz Duplaga; David Ingram. *Information Technology Solutions for Healthcare*, London: Springer, 2006.

3 Hausmann, Hannelore. *Die elektronische Gesundheitskarte kommt. Nutzen und Risiken der Telematik im Gesundheitswesen für Patienten und Gesellschaft*, Bonn: Friedrich-Ebert-Stiftung, 2006.

4 Bundesamt für Sicherheit in der Informationstechnik (BSI). *Die Lage der IT-Sicherheit in Deutschland 2007*, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2007.

5 Gigerenzer, Gerd. „Simple tools for understanding risks: from innumeracy to insight", BMJ, 327, 2003, S. 741-744; Gigerenzer, Gerd, Todd, P. M., the ABC Research Group. *Simple heuristics that make us smart*, New York: Oxford University Press, 2001.

6 Kahn, David. *The Codebreakers: The Story of Secret Writing*, New York: Scribner, 1996; Kahn, David. *Seizing the Enigma*, London: Arrow, 1996.

7 Kahn, David. *The Codebreakers*, S. 230ff.

8 gematik, *Datenschutz und Datensicherheit. Übergreifendes Sicherheitskonzept der Gesundheitstelematik*, Stand vom 10.03.2008 gültig für Release 2.3.3 und 0.5.2. Download: http://www.gematik.de/Detailseite/Datenschutz_und_Datensicherheit/Uebergreifendes_Sicherheitskonzept_der_Gesundheitstelematik.Gematik

9 Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI TR-03116 *Technische Richtlinie für die eCard-Projekte der Bundesregierung*, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2007.

10 Eckstein, L.; Parslow, H. „Health cards relevance and application fields of SmartCard technology in public healthcare", In: *GMD - Forschungszentrum Informationstechnik GmbH: 25 years GMD Darmstadt, Sankt Augustin: GMD Forschungszentrum Informationstechnik*, 1999, S.48-51; Domingo-Ferrer, Josep. *Smart card research and advanced applications*: 7th IFIP WG 8.8/11.2 international conference, CARDIS 2006, Tarragona, Spain, April 19-21, 2006, *Lecture notes in computer science*; 3928, Berlin: Springer, 2006.

IMPRESSUM

Herausgeber
gematik GmbH
Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

info@gematik.de
www.gematik.de

Tel.: 030/40041-0
Fax: 030/40041-111
Geschäftsführer: Peter Bonerz, Dirk Drees

Handelsregister: HRB 96351 B

Verantwortlich für den Inhalt
gematik

Text
Dr. Sybe Rispens, Berlin

Gestaltung
keil:scheiffele, Berlin

Infografiken
Theo Barten, Den Bosch

Druckdurchführung
duodesign, Berlin

Druck
LASERLINE
Digitales Druckzentrum Bucec & Co.
Berlin KG